(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 2003/081377 A3

(51) International Patent Classification[7]: G07F 19/00, 7/10, H04L 9/32, 9/08

(21) International Application Number: PCT/US2002/040616

(22) International Filing Date: 18 December 2002 (18.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/026,848 21 December 2001 (21.12.2001) US

(71) Applicant *(for all designated States except US)*: **ESIGNX CORPORATION** [US/US]; 19925 Stevens Creek Boulevard #109, Cupertino, CA 95014 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WANG, Ynjiun, P.** [US/US]; 10127 Linda Ann Place, Cupertino, CA 95014 (US).

(74) Agents: **SHERIDAN, James, A.** et al.; Moser, Patterson & Sheridan, L.L.P., 350 Cambridge Avenue, Suite 250, Palo Alto, CA 94306 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

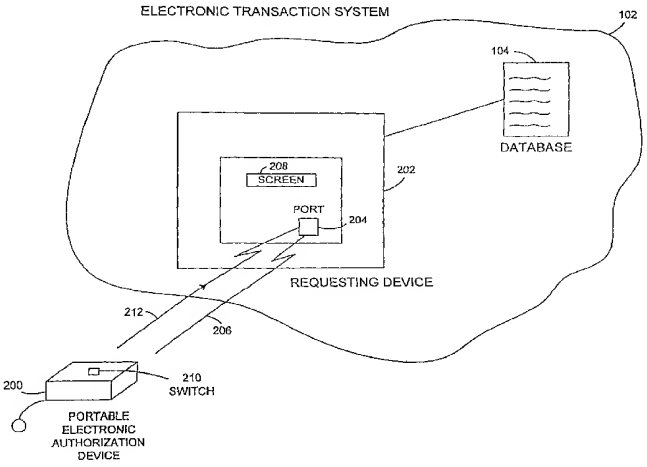
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 4 March 2004

[Continued on next page]

(54) Title: METHODS OF EXCHANGING SECURE MESSAGES



(57) Abstract: The invention enables a registered PEAD user to exchange a secure message with another registered PEAD user by using the user ID and the user public key information in the server. The sender can retrieve the public key information from the server 1201 using the receiver's user ID as an index; then the sender can derive the shared secret using the receiver's public key. The sender then can encrypt the message with the shared secret and send it over to a server with the other PEAD user's (receiver's) ID appended with the sender's user ID over the wireless network and/or Internet. The server then stores the message and forwards the message to the receiver once the receiver's PEAD is polling for messages. (It is understood in the art that the server can push the messages to the receiver's PEAD). The receiving PEAD user can use the sender's PEAD user ID and sender's public key information to derive the shared secret to decrypt a received secure message. Once a shared secret is computed or established by protocol between two users, that shared secret can be saved in the PEAD for future communication encryption/decryption usage.

WO 2003/081377 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/40616

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G07F7/10 H04L9/32 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 25371 A (Y. WANG) 11 June 1998 (1998-06-11) abstract; claims; figures	1-4
A	US 5 956 402 A (KIEM-PHONG VO) 21 September 1999 (1999-09-21) abstract; claims; figures	1-4,6,13
A	WO 99 57844 A (CERTICOM) 11 November 1999 (1999-11-11) abstract; claim; figures	1,2,5,15
A	US 5 920 630 A (M.A. WERTHEIMER ET AL.) 6 July 1999 (1999-07-06) abstract; claims; figures	1,2,5-8, 12,15-17
A	US 6 094 487 A (T. BUTLER ET AL.) 25 July 2000 (2000-07-25)	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 January 2004	15/01/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/US 02/40616

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 39476 A (CERTICOM) 5 August 1999 (1999-08-05)	
A	US 5 748 735 A (R. GANESAN) 5 May 1998 (1998-05-05)	
A	WO 98 39745 A (DEUTSCHE TELEKOM) 11 September 1998 (1998-09-11)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 02/40616

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9825371	A	11-06-1998	US	5917913 A	29-06-1999
			AU	5383198 A	29-06-1998
			US	6282656 B1	28-08-2001
			WO	9825371 A1	11-06-1998
			US	6594759 B1	15-07-2003
			US	6175922 B1	16-01-2001
			US	2002023215 A1	21-02-2002
US 5956402	A	21-09-1999	WO	9839877 A1	11-09-1998
WO 9957844	A	11-11-1999	CA	2236495 A1	01-11-1999
			US	2001016908 A1	23-08-2001
			AU	3590299 A	23-11-1999
			WO	9957844 A1	11-11-1999
			EP	1075746 A1	14-02-2001
			JP	2002514841 T	21-05-2002
US 5920630	A	06-07-1999	NONE		
US 6094487	A	25-07-2000	NONE		
WO 9939476	A	05-08-1999	AU	2145999 A	16-08-1999
			CA	2320221 A1	05-08-1999
			WO	9939476 A1	05-08-1999
			EP	1050134 A1	08-11-2000
			JP	2002502186 T	22-01-2002
			US	6430690 B1	06-08-2002
US 5748735	A	05-05-1998	US	5557678 A	17-09-1996
			US	5535276 A	09-07-1996
			US	5838792 A	17-11-1998
			US	5737419 A	07-04-1998
WO 9839745	A	11-09-1998	WO	9839745 A2	11-09-1998
			EP	0970449 A2	12-01-2000
			HU	0004242 A2	28-05-2001
			NO	994235 A	28-10-1999